DIABETES TECHNOLOGY SOCIETY

DTMoSt

Diabetes Technology Society (DTS) is pleased to announce that the steering committee members of the Diabetes Technology Society Mobile Platform Controlling a Diabetes Device Security and Safety Standard (DTMoSt) project have developed the **DTMoSt Guidance for Use of Mobile Devices in Diabetes Control Contexts.**

PRESS RELEASE

New Standard Provides Security Guidance for Consumer Mobile Phones Controlling Diabetes Devices

May 22, 2018 – Burlingame, CA – Diabetes Technology Society (DTS) today announced the first official public release of DTMoSt, a consensus cybersecurity standard whose goal is to provide assurance that consumer mobile phones can safely control diabetes devices.

Today, dozens of companies have developed mobile apps to help people monitor their diabetes. Soon, smartphones will also enable patients and healthcare professionals to directly manage care, including the use of apps as remote controls for insulin delivery. DTMoSt aims to ensure that sufficient security measures are taken to protect the integrity of these control solutions and the safety of patients with diabetes.

The DTMoSt Guidance builds upon the DTS Cybersecurity Standard for Connected Diabetes Devices (DTSec), which is the first consensus cybersecurity standard for connected diabetes devices with US government input. DTMoSt will be the first standard with both performance requirements and assurance requirements for manufacturers of connected medical devices controlled by a mobile platform. DTMoSt identifies threats, such as malicious remote and app-based attacks and resource starvation, to the safe operation of mobile device-enabled solutions and offers guidance to developers, regulators, and other stakeholders to help manage these risks.

Today, the public lacks visibility into and assurance for the security properties of connected devices," said David Kleidermacher, Vice President - head of security for Android, Chrome OS, and Play at Google, and the standard's Steering Committee technical chair. "DTMoST enables the application of a kind of security nutrition label, based on independent expert security evaluation, that is keenly needed to fill this gap, especially in critical solutions such as mobile-controlled medical care."

"CyberSafety by-Design is integral to our Omnipod connected digital diabetes innovations at Insulet," said Dr. Aiman Malek, Executive Vice President and Chief Technology Officer at Insulet. "The DTMoSt Guidance provides the cybersecurity blueprint to help address the diabetes community's request to build mobile applications that provide safe control of their pumps."

Anura Fernando, Principal Engineer – Medical Systems at UL, said "UL is glad to be a part of this effort focused on bringing more attention to the security issues that are driven by specific clinical use cases in diabetes management."

The standard was open to public comment for 45 days, from February 7, 2018 through March 24, 2018.

AVAILABILITY

DTMoSt, The Diabetes Technology Society Guidance for Mobile Platforms Controlling a Diabetes Device Security and Safety Standard is available at https://www.diabetestechnology.org/dtmost.shtml

DTSec, The Diabetes Technology Society Cybersecurity Standard for Connected Diabetes Devices and the Diabetes Technology Society Protection Profile for Connected Diabetes Devices are available at https://www.diabetestechnology.org/dtsec.shtml